

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Milwaukee Fire Department Firehouse located at
3529 S. 84th Street, Milwaukee, Wisconsin

)
)
)
)
)
)

Case No. 17-M-1214

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 2252 and 2252A

The application is based on these facts: See attached affidavit.

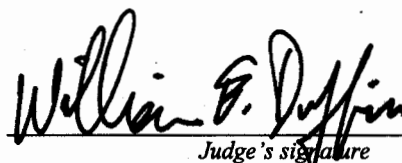
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Jason B. Pleming, Special Agent
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 2/8/17


Judge's signature

City and State: Milwaukee, Wisconsin

Case 2:17-mj-01214-WED Filed 05/02/17 Page 1 of 29 Document 1

William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

ATTACHMENT A

DESCRIPTION OF THE PROPERTY TO BE SEARCHED

The Subject Premises is a Milwaukee Fire Department ("MFD") Firehouse located at 3529 S. 84th Street, Milwaukee, Wisconsin. The MFD Firehouse at this location is Station 29 and is located in the 3rd Battalion. Further, this station houses Engine 29. Station 29 is more specifically described as the following: a red brick building with three overhead doors in the front of the building. To the left of the overhead doors is the main entrance to the station. The main entrance has a glass entry door. To the right of the entry door is a glass window where the numerals "3529" are visible in white lettering. Above the entry door and window, the text "Milwaukee Fire Department" is visible in silver lettering.

#

ATTACHMENT B

Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses; and

- m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes

described above including

- a. Records, information, and items relating to the occupancy or ownership of the Subject Premises, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
- c. Records and information relating to sexual exploitation of children, including correspondence and communications.

6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing);

any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

#

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Jason B. Fleming, being first duly sworn, hereby depose and state as follows:

Background

1. I am a Special Agent with the FBI and have been a sworn law enforcement officer since 2006. I am assigned to the FBI's Child Exploitation Task Force, Milwaukee Division, City of St. Francis, Wisconsin.

2. As part of my duties as an FBI Special Agent, I am authorized to investigate violations relating to child exploitation and child pornography, including the receipt, possession, and distribution of child pornography, in violation of 18 U.S.C. § 2252, and 2252A. I have gained experience in conducting these investigations through training and through my everyday work as an FBI agent. My work includes executing search warrants and conducting interviews of individuals participating in the trading and manufacturing of child pornography. I also received training relating to the investigation of Internet Crimes Against Children ("ICAC"), including training in the investigation and enforcement of state and federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.

3. The facts contained in this affidavit are based on my personal knowledge, including what I have learned through my training and work experience, as well as information I have obtained from other law enforcement officers, who have provided information to me in the course of their official duties and whom I consider to be truthful

and reliable. Some of the information was provided in response to administrative subpoenas. I also believe this information to be reliable.

4. I make this affidavit in support of an application for a warrant to search the Milwaukee Fire Department ("MFD") Firehouse located at 3529 S. 84th Street, Milwaukee, Wisconsin, as further described in Attachment A (the "Subject Premises"), for evidence, instrumentalities, and contraband, described further in Attachment B, concerning violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography) (the "Subject Offenses").

5. Because I am submitting this affidavit for the limited purpose of obtaining a warrant, I have not set forth in this affidavit everything I know about this matter.

Definitions

6. The following definitions apply to this affidavit and Attachment B to the search warrant application:

7. **Internet:** The Internet is a global network of computer systems that allows individual computers¹ to communicate through a set of established protocols. In order to

¹ The term "computer" includes routers, switches, smart phones, portable digital assistants, game consoles, and other electronic devices that have the ability to communicate with another device over the Internet.

communicate effectively over the Internet, computers are assigned a unique identifier known as an Internet Protocol ("IP") address. Every device connected to the Internet has an assigned unique IP address that allows it to communicate with other devices.

8. ***Internet Protocol ("IP") address:*** An IP address is a unique numeric address used by computers on the Internet. As used in this affidavit, an IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned a unique IP address so that Internet traffic sent to and from that computer may be directed properly from its source to its destination.

9. ***Peer-to-peer ("P2P"):*** P2P is a file sharing method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file-sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file-sharing network, a user first obtains a P2P client software program for a particular P2P file-sharing network, which can be downloaded from the Internet. In general, P2P client software allows the user to set up a file or files on a computer to be shared on a P2P file-sharing network with other users running compatible P2P client software. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. The advantage of such

multiple-source downloading that it speeds up the time it takes to download the file. It is also possible to download the file or files from only one computer.

10. **Hash Algorithm:** Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value (*i.e.*, MD5, SHA-1, eD2K, and MD4) is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. The slightest alteration of any file will result in a completely different hash value. By using a hash algorithm to uniquely identify files on a P2P network, the network efficiency is greatly improved. Because of this, typically, users may download a selected file from numerous sources by accepting different segments of the same file from each source and then reassembling the complete file on the local computer. This is referred to as multiple-source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

11. **BitTorrent P2P Network:** The BitTorrent network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide

files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs. Examples of such P2P client software programs include the BitTorrent client program, uTorrent client program, and Vuze client program. Such P2P client software programs are publically available, can be downloaded from the Internet, and are typically free. BitTorrent sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The torrent websites do not contain the files being shared; instead, they only the file known as a "torrent." These torrent websites will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referenced in the torrent file, the file(s) size, and the "info hash" SHA-1 value of the torrent file. A user may then select a torrent file(s) from the search results for download. For example, a person interested in obtaining child pornographic images/videos could open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a torrent from the results displayed the file(s) he/she wants to download. Once the torrent file is downloaded, it is used by a BitTorrent program, which the user had previously installed. The file(s) is downloaded directly from the computer or computers sharing the file. The users can receive pieces of the selected file from numerous sources at once. Once received, the pieces are then reassembled into the entire selected file. The downloaded file(s) is stored in an area

(folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file will remain in that folder until moved or deleted. Like other P2P file-sharing programs, BitTorrent allows for multiple files to be downloaded at the same time.

Facts Supporting Finding of Probable Cause

12. On July 30, 2016, I searched for the info hash 99a33c40f2fa35910d816a974db1dfacbb9b239d, which I knew to contain child pornography images based on a list of known info hashes previously identified through other unrelated FBI investigations.² This torrent file defines three files, at least one of which was identified as relating to other federal child pornography investigations.

13. On or about July 30, 2016, between 1414 hours UTC³ and 1603 hours UTC, I successfully downloaded the three files identified by info hash 99a33c40f2fa35910d816a974db1dfacbb9b239d that a device at IP address 72.128.112.11 was making available. The device at IP Address 72.128.112.11 was the sole candidate for each download, and as such each file was downloaded directly from this IP Address. I was directly connected to a device at IP address 72.128.112.11 during the download. The device at IP address 72.128.112.11 reported that it was using BitTorrent client software -UT340B- uTorrent 3.4.

² As described above, the info hash is a unique identifier for a particular file. Therefore, an info hash that was identified during an earlier investigation as relating child pornography is known to contain the same file content. Based on my training and experience, I know that if the file content changes, the info hash will also change.

³ UTC represent "Coordinated Universal Time," and is 6 hours ahead of Central Time.

14. I reviewed the downloaded files obtained from the device at IP address 72.128.112.11, and determined that one of the video files depicted child pornography. The downloaded file was entitled, "Lolita pthc underage angel pedo(full movie 14 minutes).avi". A description of the file is as follows:

- This file is a video file which is approximately 14 minutes and 28 seconds in length. This video depicts a minor female dancing and posing throughout the video. The minor female is completely naked throughout the majority of the video dancing and posing in sexually suggestive poses. The minor female's vagina is exposed numerous times during the video and is the focus of the camera.

15. On or about August 1, 2016, I focused my investigation on a device at IP address 72.128.112.11, because it was associated with a torrent with the info hash b4dc3c7c5031aacfc9c22c84c588b14794356cae, which I knew to contain child pornography based upon a list of known info hashes previously identified through other unrelated FBI investigations. This torrent file defines 774 files, at least one of which was identified as relating to other federal child pornography investigations.

16. On or about August 1, 2016, between 0127 hours UTC and 0622 hours UTC, I successfully downloaded 412 files of the 774 files identified by info hash b4dc3c7c5031aacfc9c22 c84c588b14794356cae that a device at IP address 72.128.112.11 was

making available through BitTorrent. The device at IP Address 72.128.112.11 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The device at IP address 72.128.112.11 reported it was using BitTorrent client software -UT340B- uTorrent 3.4.

17. I reviewed all 412 image files downloaded from the device at IP address 72.128.112.11, which depicted minors in different stages of undress and in sexually suggestive poses. I performed cursory review of the 412 images and identified over 50 images of child pornography. The following two files are representative examples of the child pornography files:

- a. File name: ism-016-051.jpg – this file is an image file. The image depicts a prepubescent female completely naked with her legs spread exposing her vagina.
- b. File name: t-005-61.jpg – this file is an image file. The image depicts a prepubescent female is wearing a pink colored costume which is open in the front. The prepubescent female's chest and vagina are exposed. Further, her legs are spread apart exposing her vagina.

18. I reviewed the undercover download logs for the above described download activity and noted the IP address 72.128.112.11 used port 6881 for all of the downloads. It should be noted port 6881 is commonly associated with BitTorrent traffic.

19. On or about July 30, 2016 and again on August 1, 2016, I queried IP address 72.128.112.11 through the American Registry for Internet Numbers ("ARIN") ARIN

reported IP address 72.128.112.11 is registered to Time Warner Communications ("TWC"). ARIN operates a publicly available website that lists contact and registry information for domain names and IP addresses.

20. On or about August 5, 2016, an administrative subpoena was sent to TWC requesting subscriber information for IP address 72.128.112.11 on August 1, 2016, during the download activity described above.

21. On or about September 14, 2016, TWC, produced records in response to the subpoena. According to TWC records, IP address 72.128.112.11 was subscribed to the Subject Premises on the date and time during the download activity described in paragraphs 15-18.

22. On October 13, 2016 United States Magistrate Judge David E. Jones authorized the installation and use of a pen register and a trap and trace device and process ("pen-trap device") on internet account subscribed to the Subject Premises.

23. On or about December 12, 2016, I reviewed the data obtained from the pen-trap device on the internet account at the Subject Premises. According to data obtained through the pen-trap device, I identified computer network traffic between IP address 72.128.112.11 and the IP address used by the FBI on December 9, 2016.

24. I then queried FBI MW's undercover downloads for the IP address 72.128.112.11 on December 9, 2016. From this query, I located additional downloads from IP address 72.128.112.11 that contained apparent child pornography images. Based on my training and experience, I know that BitTorrent traffic uses port 6881 predominantly.

25. On or about January 15, 2017, I focused my investigation on a device at IP address 72.128.112.11 because it was associated with a torrent with the info hash d6259150a57df3d21148a701bfebf2761496e4a4, which I knew to contain child pornography based upon a list of known info hashes previously identified through other unrelated FBI investigations. This torrent file defines seven files, at least one of which was identified as relating to other federal child pornography investigations.

26. On January 15, 2017, between 0220 hours UTC and 0510 hours UTC, I successfully downloaded the seven files identified by info hash d6259150a57df3d21148a701bfebf2761496e4a4 that a device at IP address 72.128.112.11 was making available. The device at IP Address 72.128.112.11 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The following are the seven files I downloaded:

- a. Little Pearl-016a.rar
- b. Lolita Arina-05.avi
- c. LS touch-008a.rar
- d. LS touch-020a.rar
- e. Showgirls.02.rar
- f. Showgirls.16.rar
- g. Showgirls.21.rar⁴

⁴ Of the seven files shown above, six contained the file extension ".rar". The ".rar" file format typically denotes that those files are compressed, in a manner similar to ".zip" compressed files.

27. On January 30, 2017, I used a commercial available computer program to uncompress the six ".rar" files. After that, I noted the following number of files within each of the six compressed (.rar) files:

- a. Little Pearl-016a.rar – This compressed file contained 103 image files. All 103 files depicted a prepubescent minor in different stages of undress and in sexually suggestive poses. During a cursory review of the images, I identified at least 15 images of child pornography.
- b. LS touch-008a.rar - This compressed file contained 98 image files. All 98 files depicted a prepubescent minor in different stages of undress and in sexually suggestive poses. During a cursory review of the images, I identified at least 13 images of child pornography.
- c. LS touch-020a.rar - This compressed file contained 93 image files. All 93 files depicted a prepubescent minor in different stages of undress and in sexually suggestive poses. During a cursory review of the images, I identified at least 14 images of child pornography.
- d. Showgirls.02.rar - This compressed file contained 109 image files. All 109 files depicted a female in different stages of undress and in sexually suggestive poses. At this time, I cannot confirm whether this female is a minor.
- e. Showgirls.16.rar - This compressed file contained 103 image files. All 103 files depicted a prepubescent minor in different stages of undress

and in sexually suggestive poses. During a cursory review of the images, I identified at least 13 images of child pornography.

- f. Showgirls.21.rar - This compressed file contained 101 image files. All 101 files depicted a minor in different stages of undress and in sexually suggestive poses. During a cursory review of the images, I identified at least 19 images of child pornography.

28. The remaining file, "Lolita Arina-05.avi" is a video file. This video file is approximately four minutes and 59 seconds in length. The minor female begins the video fully clothed on top of a bed, but immediately begins to take off all of her clothes. The minor female's vagina is exposed numerous times during the video and is the focus of the camera.

29. On December 21, 2016, United States Magistrate Judge William E. Duffin signed a 60-day extension to the existing pen-trap device at the Subject Premises.

30. Based on the undercover session detailed in paragraphs 25 through 31, I reviewed the data from the pen-trap device and I identified network traffic between IP address 72.128.112.11 and FBI MW's undercover IP address on January 15, 2017. In addition, I observed IP address 72.128.112.11 utilizing port 6881 during these connections for the time period when the child pornography files were obtained from the device at 72.128.112.11.

31. On or about January 31, 2017, Task Force Officer Sean Lips conducted a wireless survey in the vicinity of the Subject Premises. During this survey, TFO Lips

observed three secured wireless access points ("WAP") named, "FIREMAN29," "FIREMAN29HD," and "MFDWIFI." Based on the names of the WAPs, I believe them to be associated with the Subject Premises. Additionally, based on my training and experience, because they are secured WAPs, I know that an individual using one of those secured WAPs would have to enter in a password before being allowed to connect a computer to the WAP. In other words, these secured WAPs were password protected so they were not accessible to the general public.

Computers, Electronic Storage, and Forensic Analysis

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. *Probable cause.* I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a

storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
- e. For the reasons stated above in paragraphs 15 through 21, there is reason to believe that there is a computer system currently located on the Subject Premises.

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, and can thus enable the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The

existence or absence of anti-virus, spyware, and malware detection programs can indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, can also indicate the presence of additional electronic storage media (*e.g.*, a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer can provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer might indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a

computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) might be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet

discussions about the crime; and other records that indicate the nature of the offense.

35. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing

that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

37. The vast majority of the download activity from the Subject Premises has taken place between 8:00 p.m. to 4:00 a.m. Additionally, based on a review of work schedules for employees at the Subject Premises obtained from the Milwaukee Fire Department, I believe the person responsible works on the "Green" squad. According to information obtained from the Milwaukee Fire Department, employees assigned to the "Green" squad will next work at the Subject Premises from 8:00 a.m. on Friday, February 10, 2017, until 8:00 a.m. the following day.

38. The FBI plans to monitor real-time data from the pen-trap device installed on the TWC internet service at the Subject Premise during the period specified in the paragraph above. In addition, the FBI plans to monitor the wireless internet activity at the Subject Premise from a mobile pen-trap device. If, at that time, the FBI identifies internet activity over port 6881 from IP address 72.128.112.11 and/or identifies additional information that suggests child pornography is being distributed the warrant will be executed.

39. For those reasons, I submit that good cause exists to allow the warrant to be executed any time in the day or night and outside daytime hours

Conclusion

40. For these reasons, I submit that the evidence and information set forth in this affidavit provides probable cause to believe (a) that someone employed at the Subject Premises described in Attachment A to the search warrant application has committed the crime of distributing child pornography, in violation of Title 18, United States Code, Section 2252(a)(2) and (b) that evidence relating to that crime, described in Attachment B to the search warrant application, can be found at the Subject Premises.

#